



A Europa Clipper, Integrated Model-Centric Engineering (IMCE), and Safety and Mission Assurance (SMA) partnership

Model-based Probabilistic Risk Assessments (PRA)

MBMA Workshop #2

Josh Bendig

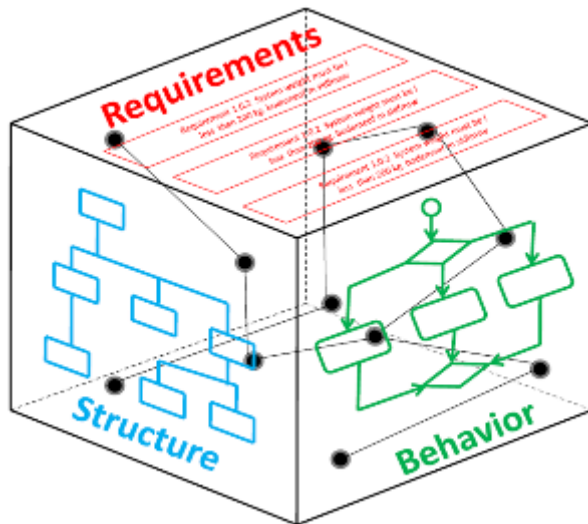
May 7, 2019

Acknowledgements: Kelli McCoy, Chet Everline



Jet Propulsion Laboratory
California Institute of Technology

What is MRAP? Mission Risk Assessment Plan



System Model



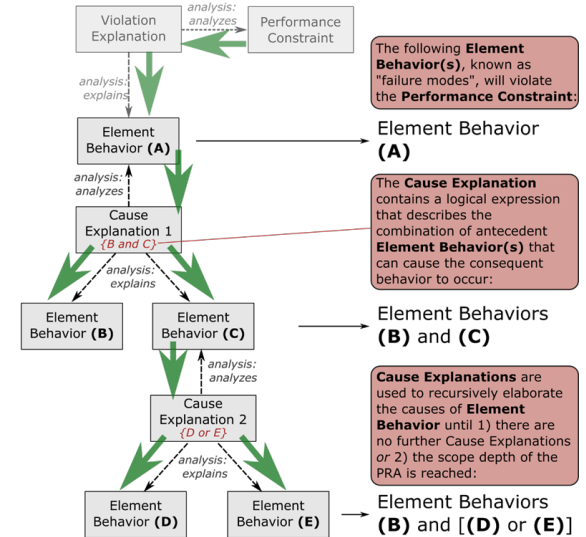
Violation Explanations explain how certain **Element Behavior** violates the **Performance Constraint** being analyzed.

Element Behavior that violates a **Performance Constraint** is considered a "failure mode".

Cause Explanations analyze **Element Behavior(s)** and explain why other **Element Behavior(s)** may cause it.

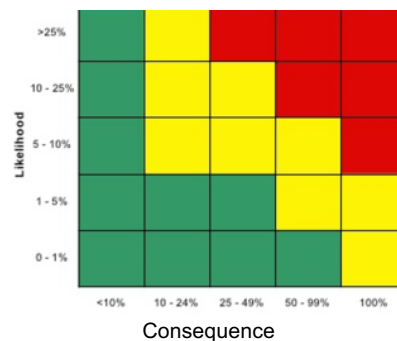
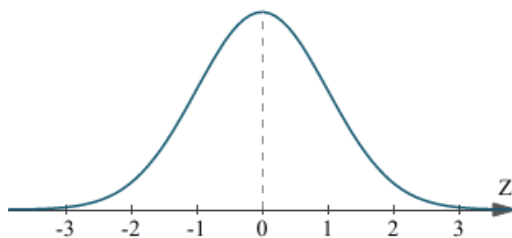
Element Behavior that is not analyzed by a **Cause Explanation** has no identified causes, which classifies it as "basic behavior" (i.e. Element Behavior B).

The PRA methodology recursively traverses through **Cause Explanations** to locate basic **Element Behaviors**. The occurrence of a basic behavior is considered a basic event.

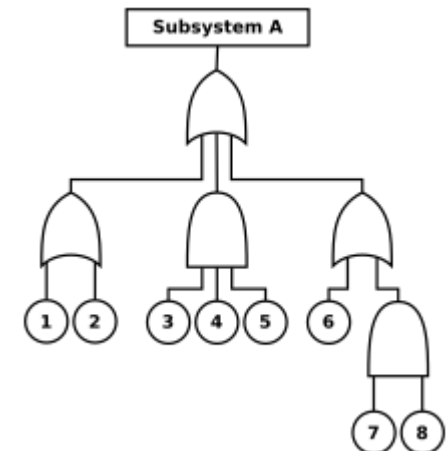


IMCE PRA scripts

Europa's MBSE infrastructure + IMCE's PRA script development = unique opportunity to pursue a novel approach to performing PRAs



Probabilistic Risk Assessment

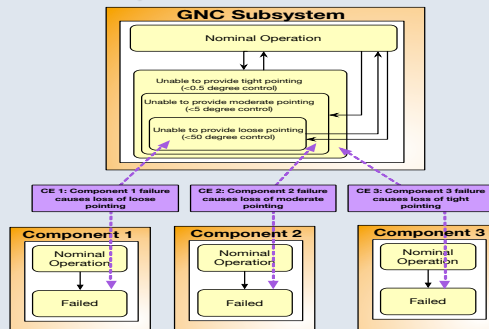


MBSE PRA Process

Develop foundational capability to perform Probabilistic Risk Assessments (PRAs) from a System Model



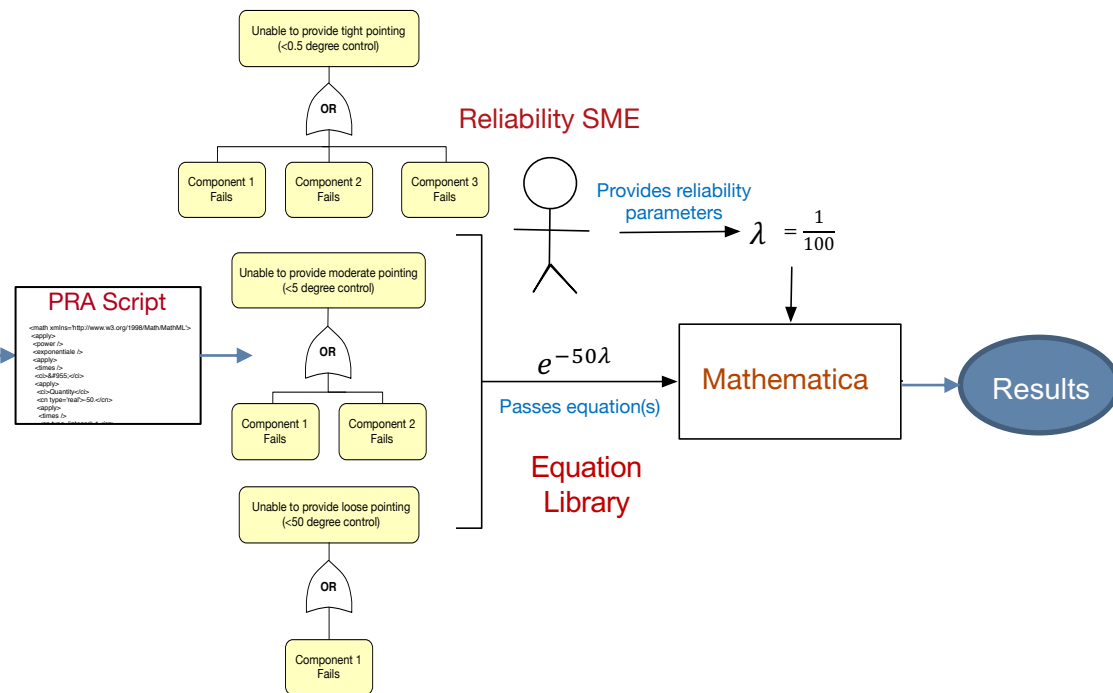
Design Capture Model: components, causal dependencies, state machines



Box-level modeling now in place

Timeline Management System: Operational Scenarios

SCET	2024-355T00:00:00	2024-356T00:00:00	2024-357T00:00:00	2024-358T00:00:00	2024-359T00:00:00	2024-360T00:00:00
MissionSubPhase	2024-12-20 00:00:00	2024-12-21 00:00:00	2024-12-22 00:00:00	2024-12-23 00:00:00	2024-12-24 00:00:00	2024-12-25 00:00:00
GNCMode	EARTH1				INERTIAL	DE
Inertia_Measurement	On_Full_Power					
Inertia_Measurement	On_Full_Power					



The use of a single source of truth enables a consistent foundation across all PRAs.

MRAP Documentation

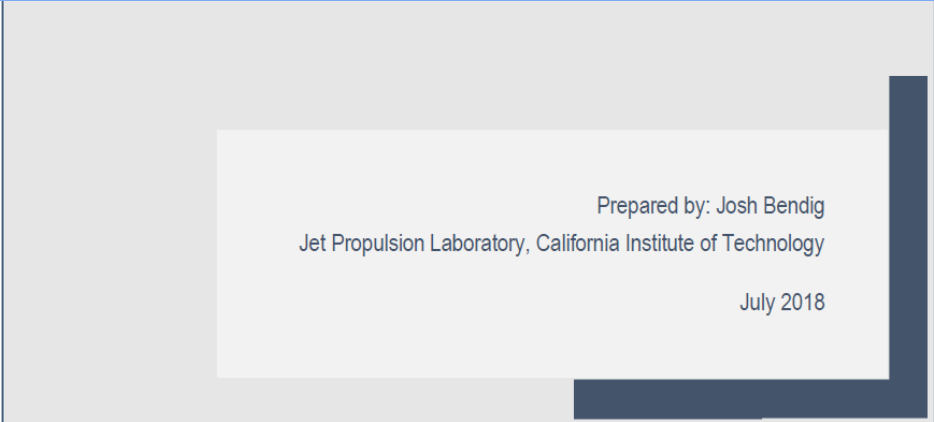


Model-Based Probabilistic Risk Assessment (PRA) USER GUIDE

Documentation was developed to help other missions implement a similar process

Additional Public references:

1. Schreiner, S., et al. *"Towards a methodology and tooling for Model-Based Probabilistic Risk Assessment (PRA)."* AIAA Space 2016.
2. Castet, J. F., et al., *"Fault Management Ontology and Modeling Patterns."* AIAA Space 2016. Long Beach, CA, 2016.
3. Castet, J. F., et al. *"Ontology and Modeling Patterns for State-Based Behavior Representation,"* Infotech @ Aerospace, AIAA SciTech, Kissimmee, Florida, 2015.



Prepared by: Josh Bendig
Jet Propulsion Laboratory, California Institute of Technology

July 2018

Traditional vs MRAP Approach

System modeling:

- understanding the system elements to be modeled;
- modeling how failures in these elements (leaf-level events) cause functional failure;
- identifying risk scenarios and modeling their occurrence probability;
- acquiring reliability data.

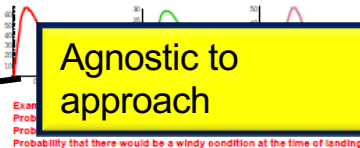
Should already be in the system model.

Added to system model through cause & violation explanations

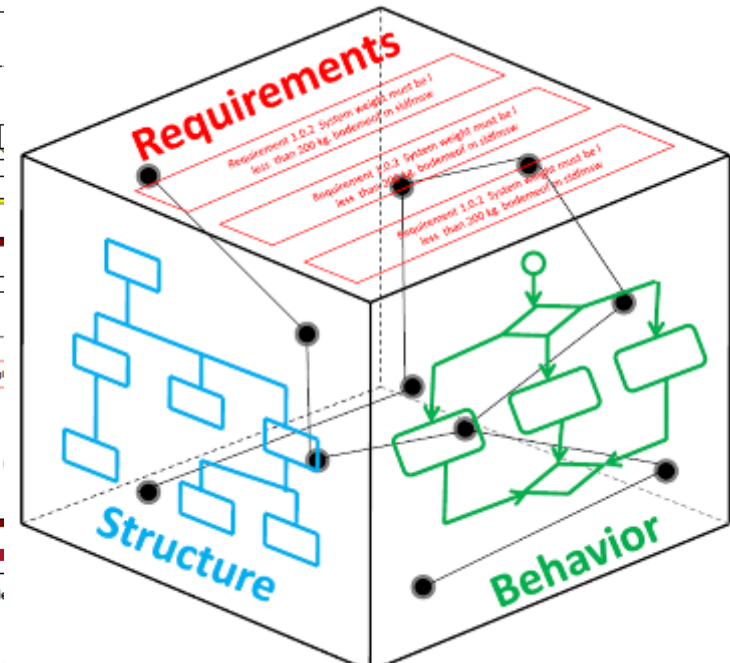
PRA script and Equation Library

Agnostic to approach

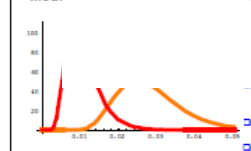
Probabilistic Treatment of Basic Events



The uncertainty in occurrence of an event is characterized by a probability distribution



Model



scenario in terms of basic events

likelihood of risk scenarios

uncertainty in the likelihood estimate

- human errors, etc./
- Insights into how various systems interact
- Tabulation of all the assumptions
- Identification of key parameters that greatly influence the results
- Presenting results of sensitivity studies

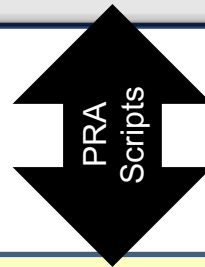
Using the MRAP approach, there were roughly 3 PRAs developed (for the Europa Clipper mission) for the cost of 1 PRA, using traditional methods

Example Application: Europa Clipper PRAs

Europa Clipper PRAs of interest

Europa System Model/TMS

Hardware
Requirements
State transition timelines / Operational Scenarios
Causal Dependencies



MRAP

Planetary Protection

Study Outcome:
Probability of
Contamination

Performing greater microbial reduction will not improve probability of contamination (increased bioburden reduction decreases reliability)

Science Sensitivity

Study Outcome:
Probability of Meeting L1
Science Objectives

A non-driving flyby recovery capability (hours, not min) is needed to preserve science in the presence of expected outages

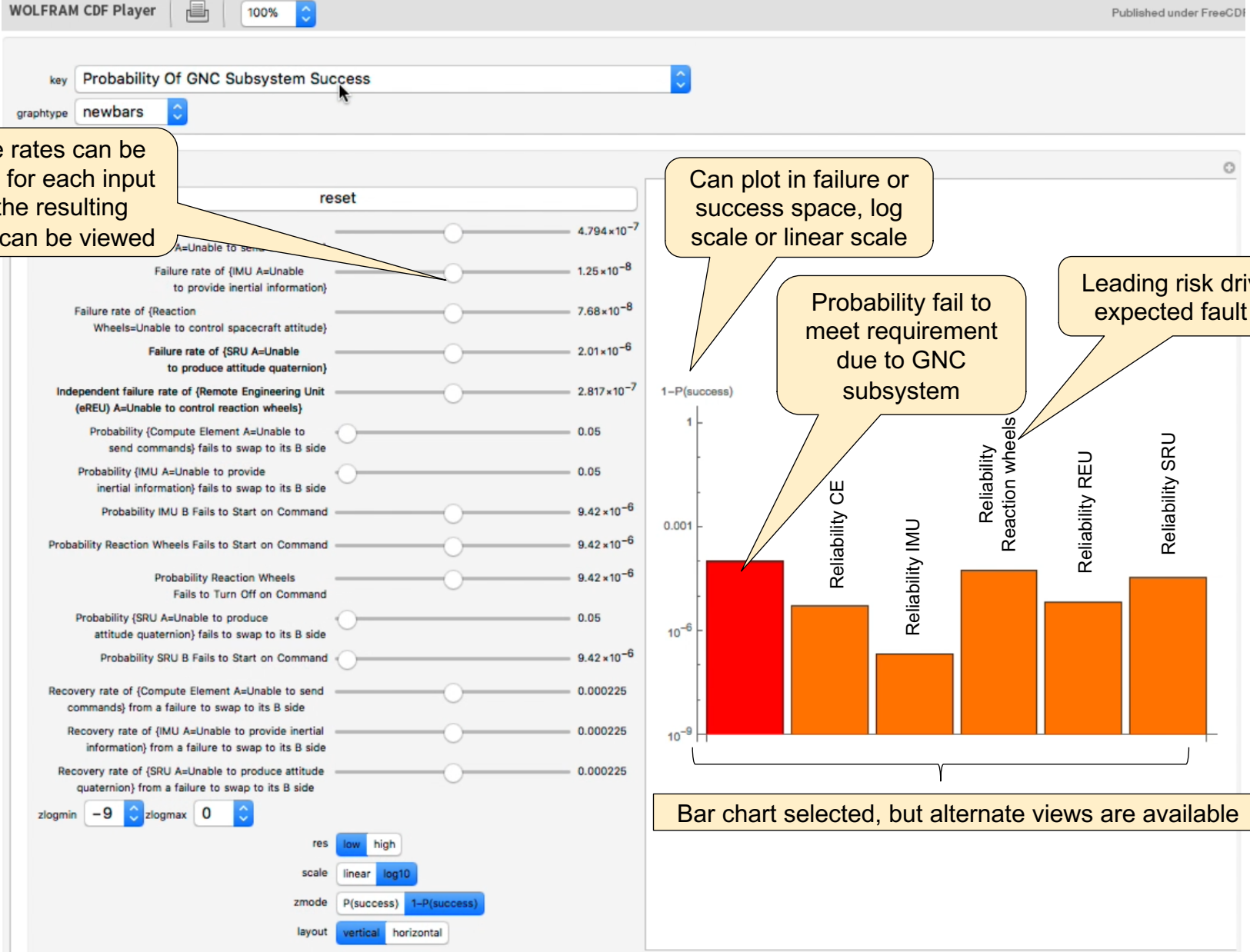
JOI Achievement

Study Outcome:
Probability of Successful
JOI

A requirement on the time duration of JOI was unnecessarily confining fault protection recovery strategies during the burn

Notable contribution

Result Analysis: Assessing Drivers of Unreliability

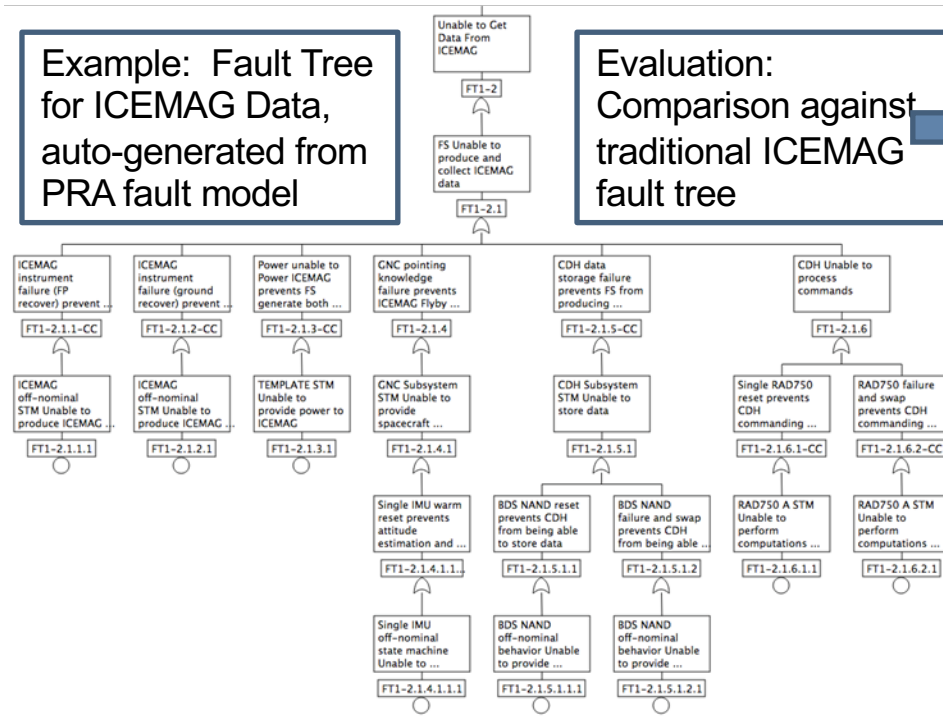


Visualization and Validation

System-generated graphics are used to validate results

Example: Fault Tree for ICEMAG Data, auto-generated from PRA fault model

Evaluation: Comparison against traditional ICEMAG fault tree



Proper FTA Node	Addressed in PRA	PRA Node ID	Notes
Failure to acquire valid data from ICEMAG	Yes	FT1.2	Head node
ICEMAG provides no data	Rolled up	(FT1.2)	Part of head node
ICEMAG is broken	Yes	FT1.2.1.1	Distinct node
Science path is broken or stuck	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
Data path is broken or stuck	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
ICEMAG is not powered	Covered		Only switch faults are modeled
Spacecraft power fault	Handled in safing		S/C wide power faults are assumed to trigger safing
ICEMAG circuit is not energized	Yes	FT1.2.1.3	Distinct node
ICEMAG command is not executed	Covered		
ICEMAG fails to respond to command	Yes	TX	Transition failure is modeled explicitly
ICEMAG data path is damaged	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
ICEMAG is latched	Rolled up	TX	Part of transition failure
C&DH fails to emit correct command	Covered		
C&DH causes safing	Handled in safing		double fault etc. assumed to trigger safing
C&DH is in reset or swap	Yes	FT1.2.1.6.1, FT1.2.1.6.2	Distinct nodes
C&DH is otherwise functional but cannot emit commands	Rolled up	(FT1.2.1.6.1, FT1.2.1.6.2)	"Other" C&DH fault rate rolled into reset / swap rates
Execution Engine is stuck or in reset	Rolled up	(FT1.2.1.6.1, FT1.2.1.6.2)	
Execution Engine has a bad sequence	Rolled up	(FT1.2.1.6.1, FT1.2.1.6.2)	
Sequence itself is bad	No	(FT1.2.1.6.1, FT1.2.1.6.2)	Command faults should be treated separately
ART sequence is bad	No	(FT1.2.1.6.1, FT1.2.1.6.2)	Probably roll up into command faults when available
ICEMAG provides bad data	Rolled up	(FT1.2)	Part of head node
Science path is broken or stuck	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
ICEMAG is cold	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
Thrusters are firing	Covered		
Spontaneous firing	Not credible		
GNC in an RCS mode	Handled in safing		Assumed unplanned thruster firing can only result from safing
Electrical power / EMI	Covered		
Spacecraft fails to provide clean power	Rolled up	FT1.2.1.3	Part of ICEMAG circuit is not energized
ICEMAG short	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
Propulsion module EMI	No		Very tricky to estimate
Other EMI	No		Very tricky to estimate
ICEMAG sends data at unexpected rate	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
ICEMAG command not executed [see above]	Covered		
ICEMAG pointing is unknown	Yes	FT1.2.1.4	Distinct node
GNC data not provided	No		Intercom rolled into C&DH failures
Intercom broken	No		Intercom rolled into C&DH failures
GNC unpowered or resetting	No		General GNC failure rolled into C&DH failures
GNC estimate invalid or missing	Yes	FT1.2.1.4.1	Distinct node
GNC sensors broken	Yes	FT1.2.1.4.1.1	Distinct node
GNC estimator broken	No		Difficult to model -- "All Other GNC Fault" node temporarily removed
ICEMAG data not transferred to Spacecraft	Rolled up	(FT1.2)	Focused on BDS story
ICEMAG data path broken	Rolled up	(FT1.2.1.1)	Part of ICEMAG is broken
Intercom broken	No		Intercom rolled into C&DH failures
BDS failure	Yes	FT1.2.1.5	Distinct node
BDS unable to handle data rate	No		Roll into command failure?
BDS unable to receive any data	Yes	FT1.2.1.5.1	Distinct node
BDS unpowered	No		Roll into command failure?
BDS is full	No		Roll into command failure?
BDS is broken	Covered		
BDS NAND is broken	Yes	FT1.2.1.5.1.1, FT1.2.1.5.1.2	Distinct nodes
BDS Controller is broken	No		Roll into command failure?

Auto-Generated Instrument Fault Tree vs. Manually Generated

Summary, Observations, and Lessons Learned

- **Every detail of system cannot be modeled**
 - Model things conservatively first; if result favorable, stop!
 - Else, target high-risk areas for detailed exploration
- **Stop at box level unless specific Project question arises driving lower-level modeling**
 - Reliability information often not available at lower levels
- **Use visualization to help validate that the system model is correct**
- **Always iterate modeling, findings, and results with subject matter experts prior to delivery**
- **Always verify MRAP scripts and architecture after each revision.**